LISE-MEITNER-ALLEE 4
D - 44801 Bochum
TELEFON +49 (0) 234/43 87 02-09
TELEFAX +49 (0) 234/43 87 02-11
E-Mail info@escrypt.com
INTERNET www.escrypt com

Security Evaluation of the

Siemens Scalance S 612/613 Security Module

escrypt GmbH – Embedded Security

http://www.escrypt.com

Version:	1.2
Date:	19-Aug-05

Index

Executive Summary

The Scalance S 612/S 613 is a security module to protect the communication between automation networks and to avoid attacks to the networks. The security module provides the functionality of a firewall and a virtual private network (VPN). The system is based on the operating system VxWorks and the firewall and VPN from OpenBSD, the web server and the packet filter for layer 2 were developed by Siemens.

Reliability and robustness are the crucial aspects for an automation network. The network must remain running even in the case of failures. The aspect of data security immediately follows in importance. Security and reliability sometimes induce different objectives and get in the way of each other. These aspects were incorporated in the standard configuration. Nonetheless the security module allows a secure configuration. The device can be installed without changing the existing network.

The security module fulfils its task well and fully protects an automation network. The simplicity of the configuration is to be emphasized where the security does not suffer. The device is built in an extremely robust manner and meets the special demands of automation networks in an excellent way. In total, the Scalance module provides a higher quality than most other security modules (also outside of the industrialization engineering branch).

1 Introduction

The Siemens Scalance S 613 is a security module which protects the communication between automation networks. It provides authentication, data integrity and confidentiality and protects against data theft and data manipulation.

In automation engineering more and more components are being connected. The connection with the Office IT world offers possibilities to use known technologies from the office field for automation networks which arises threats by attacks from the external network. The protection of the automation networks is necessary in order to be resistant against malicious attacks from the external network. Figure 1 clarifies this circumstance.

Unlike the office-world, where standardized schemes such as SSL, TLS, and IPsec are applied, there are no standards providing data security of automation networks yet. The analyzed security module protects individual components and entire networks against data theft and manipulation by implementing a firewall and a virtual private network (VPN).

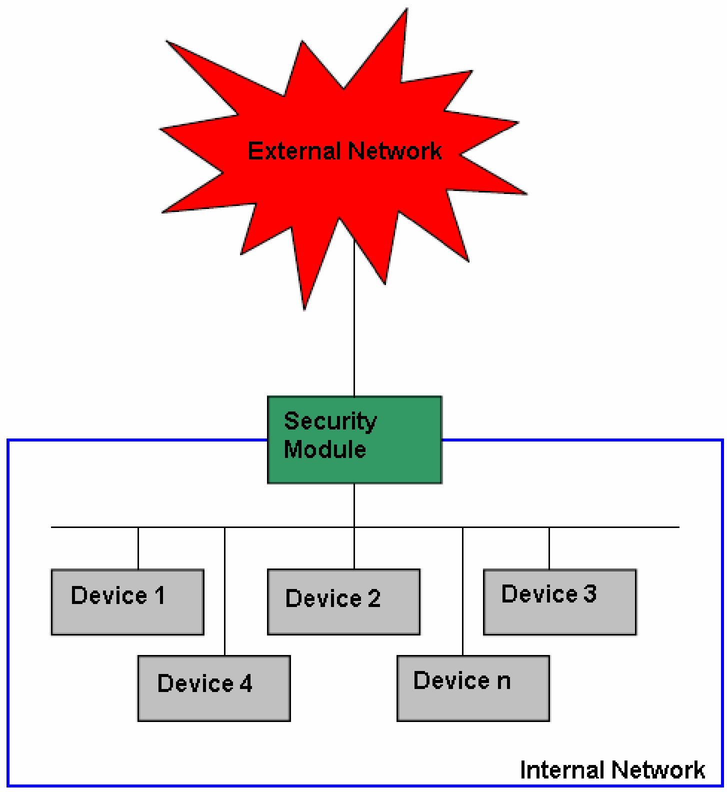

Figure 1: External network < -> internal network

Automation networks demand for a variety of security goals such that only basic default-rules are preset. Nonetheless, these default rules provide a secure configuration. The security modules are supposed to be easy to configure and handle, also by non IT-experts. The security module can still be precisely configured according to the user's requirements. With expert knowledge the configuration can be set manually in the advanced modus. The module can be installed to an existing automation network without having to change the network topology or having to configure new network nodes.

The configuration is set on a PC. It is possible to configure several security modules at the same time over the network. For the replacement of broken devices the configuration data can be stored on a removable media, the so-called C-Plug. If a broken module has to be replaced only the removable media needs to be put in the new module such that it starts working based on a secure configuration immediately.

The module is based on the operating system VxWorks of WindRiver. Some components such as packet filter and IPsec were used from OpenBSD, often quoted as the „most secure operating system". MiniWeb, a development of Siemens, is used as a HTTPs server to provide a secure communication channel for the configuration data between the configuration PC and the security modules. MiniWeb is based on OpenSSL, it uses RC4, 3DES and provides key lengths of up to 2048 bit.

Security modules can be combined in groups so that all modules of a group can communicate with each other through IPsec tunnels. The internal network nodes of a module and also of other modules can be automatically found without the need to configure them manually. The Scalance S 612 can protect a network of up to 32 internal nodes. The Scalance S 613 protects up to 64 internal nodes and has an extended temperature range of -20 ° to +70°. The computer software SOFTNET Security Client provides a secure IP-based access from a PC to subnets. The SOFTNET Security Client automatically enables a PC to communicate through a secure tunnel with a security module. The security modules are supplied by a redundant voltage supply of 24 Volts of DC voltage.

2 Security Services

The security module has two Ethernet interfaces, one to the internal network which is protected, and the other one to the external network. The interfaces are easily recognizable by a color marker in green and red color. The processor is an Intel IXP425, it supports AES, SHA-1, MD5, DES and 3DES in hardware. RSA is implemented in software.

2.1 Assumptions

Assumptions were made for the security module in a way to suffice the special needs of automation networks. The internal network is assumed to be confidential. It is assumed that the authorized users are trustworthy and are trained in order to operate the module correctly. However, the configuration is supposed to be as simple as possibly.

Furthermore, it is assumed that the module is physically secure. The module only provides a basic protection if an attacker has physical hand on the device and can exchange the device with a manipulated device or exchange the removable media.

There is no content filter available in the security module. For the protection against malicious contents such as viruses and Trojan horses, etc. a virus scanner and/or content filter must be added.

To keep the automation network running the reliability and robustness are at first place even before the security aspects. Hence, with respect to security restrictions were accepted in some default settings.

2.2 System

The security module is based on a firewall and a virtual private network (VPN). The firewall works as a packet filter and the VPN is based on IPsec. SSL is only used to protect the communication for configuration of the Scalance devices. The device incorporates a bridge that enables installing the security device without having to change any settings in the existing network regarding the IP addresses, subnet masks, and routers.

2.2.1 Firewall

In order to protect the internal network, only communication channels between devices from the external network and the internal network that are defined in advance are allowed. This task is carried out by a packet filter working on layer 2

and 3 on the security module. The packet filter controls the communication between the internal network and the external network (see Figure 2).

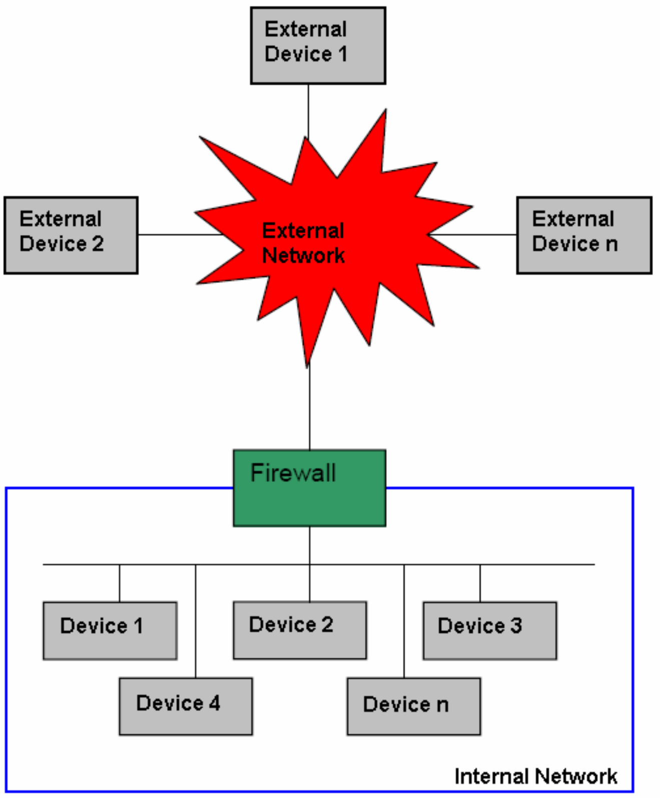

Figure 2: Firewall function of the security module

The firewall offers a packet filter adapted from OpenBSD for IP-packets with stateful packet inspection. Another packet filter for Non-IP-packets (Ethernet packets or Layer-2-packets) was developed by Siemens for the security module. There is also a bandwidth limitation in order to avoid denial of service (DoS) attacks and cache flooding.

2.2.2 VPN

The module also has the task to connect two or more internal networks to each other. This happens physically over the external network in such a way that messages from a protected device to another one are sent over the unprotected external network through a secure tunnel. In order to safeguard the confidentiality of the data, the security module can build up a VPN tunnel based on IPsec. When several bilateral tunnels are combined we call the resulting network a VPN as represented in Figure 3.

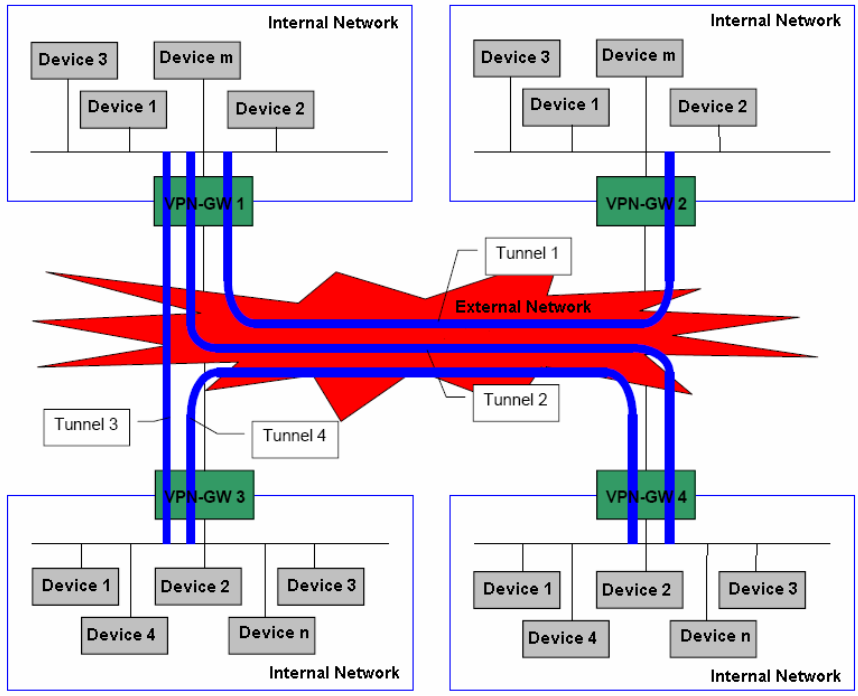

Figure 3: VPN-function of the Security-module

For the communication over a VPN the security modules are collected in groups. For each VPN there is a so called network certificate with corresponding private key that identifies the VPN. Each security module that belongs to the VPN holds a certificate which is signed with the private key of the network certificate. The network certificate is issued by a certification authority (CA) or it is self issued. The VPNs are based on IPsec and use the IKE protocol for the key management. The implementation was adapted from OpenBSD.

2.2.3 Removable Media (C-Plug)

The configuration data is stored on a removable media which is also called C-Plug. A security module can easily be configured by inserting a C-Plug storing an appropriate configuration. The configuration is then loaded by the security module and stored in the internal flash memory. The data on the C-Plug is AES encrypted. The removable media makes replacing a module very simple by exchanging the hardware device and putting in a removable media for easy configuration. The removable media is placed on the back of the module behind a cover which can only be opened with a tool. With that it is more difficult to exchange the card.

2.2.4 Firmware Update

The firmware of the security device can be updated. For this purpose, Siemens supplies an encrypted and digitally signed firmware. The user has to authenticate to the security module before loading new firmware. The new firmware is transferred to the security module via HTTPs. The signature of the firmware update is verified. If the verification is successful, the new firmware is decrypted and stored as plain data. A security module accepts only new firmware holding a correct signature. Hence, it is guaranteed that no manipulated flash software is loaded into the security module but only authentic software. The private key for computing the signature is only known to Siemens and stored in a secure way such that new firmware can only be distributed by Siemens. The corresponding public key for the verification is stored in the EEPROM of each security module. The signature of a firmware is checked at updating it, while at booting time only a checksum of the stored firmware is verified. The confidentiality of the firmware is not a security target but only a barrier if someone wants to reconstruct the firmware.

2.3 Configuration Management

Before the security module can start the work and protect an automation network, it has to be configured. A tool is used to set the parameters for the configuration of the security module including switches for the firewall, VPN, and logging. A module needs at least the IP parameters which are set automatically in the standard settings. It is possible to configure more than one module at the same time. This configuration software runs on an external PC and the configuration information is sent to the modules via HTTPs.

The configuration data is stored in the internal flash memory. The data is stored as plain data. However, during the data transmission between the configuration PC and the security module the data is securely communicated. If a C-Plug is put in the module, the data is stored encrypted in the C-Plug. They are deleted from the memory of the module after they were stored on the C-Plug.

Users with restricted rights have only a few choices to configure the module. Even non-IT-Experts are able to configure the module in such a way that failures are almost impossible. The administrator can configure the module manually in a more detailed way.

2.3.1 First Initiation

At first initialization an IP address is assigned to the Scalance S moduls. After the IP configuration the modules can also be configured over the network. The first user to take the module in operation enters a user name and password which puts him in the position of administrator.

After the security module is turned on or reset, if it does not contain any configuration data either in the internal flash or on a removable media it does not allow any communication. Hence, the device is in a state which cannot be used in any way for an attack from the external network. The communication between protected devices behind different security modules via the external network must also explicitly be approved by the configuration.

If the device needs to be reset in case of loss of passwords, there is a reset button on the back of the module. By pushing it the device is set to the delivery state. This button is protected by a cover on the back side such that it is not pushed by mistake. If the device is built in a rack, it first needs to be removed of it after the back cover can be opened.

2.3.2 User Management:

There are two user groups having different rights: The administrator and the user with restricted rights. The administrator is able to grant users access to the modules, the users are able to change configuration settings according to their rights. The authentication of the user to the security module is carried out by digest authentication with user-name and password. With this kind of authentication the password is never sent in plaintext.

2.3.3 Learning

In order to keep the configuration of the modules simple, the automatic learning was integrated. A module can learn the existence (and with that the addresses) of further modules and add this information to its own list of reachable modules. In the same way it can learn which nodes are in the internal network of another module. A VPN tunnel can only be set up if the end-point is known inducing that also the module that protects the network with that endpoint needs to be known. The learning is done automatically or by manual configuration.

For this purpose, the security module provides the security configuration protocol (SCP). This protocol contains the functions

- Find further security modules

- Exchange of addresses of the internal networks between security modules
- Signalizing that a packet was rejected because it was not received via an IPsec tunnel.

The learning is always initiated if a node wants to communicate with another node and devices located in the same subnet actively scan by ICMP messages. The exchange of information about found nodes is sent encrypted over the network.

2.4 Key Management

There are several certificates and keys used by the security module as described in the following:

- *Firmware*: In order to authenticate a new firmware for the updating process it is digitally signed with RSA. The private key is handled by Siemens only, the public key for signature verification is stored in the flash memory of each device. Additionally, the firmware to load is symmetrically encrypted with 3DES. The corresponding key is also stored in the flash memory. All devices use the same key. If the secret 3DES key is compromised, then the device must be sent to Siemens where the module is supplied with a new 3DES key.
- *SSL/configuration*: For the communication with SSL for configuration purposes a server certificate with corresponding private key is issued for each security module. If this key is compromised or the secret key is lost, the administrator needs to issue a new certificate.
- *VPN:* There are network certificates issued for each VPN. The corresponding private key is stored on the configuration PC. Every security module that belongs to the VPN holds a certificate which is signed by the secret key of the network certificate. A security module has thus a certificate with private key for every VPN it belongs to. Using this certificate it authenticates to other security modules establishing a secure communication tunnel. If a key is compromised, a new certificate must be issued with the configuration tool.
- *Configuration*: The configuration data on the removable media is encrypted with AES where a global symmetric key is used. If this key is compromised, a new global key needs to be deployed by a firmware update.

3 Security Analysis

The security module is designed for the use in automation networks. For automation networks availability and robustness are of first priority since the network must be protected against any failure so that the production never stops. For instance, in the chemical industry this is extremely important.

Of course there are also high demands regarding the data security objectives including data confidentiality, data integrity, and resistance against attacks from the external network. From the technical point of view the security module meets these high security goals. In this chapter the technical aspects will be analyzed in detail.

3.1 Network and Protocol Analysis

3.1.1 VPN

The VPN is based on the IPsec protocol family. In the last years this protocol family was established as an industrial standard for VPNs. Hence, interoperability with other systems is provided. Within this analysis the interoperability to the IPsec-implementation of the Linux kernel 2.6.x was confirmed. For the VPN functionality the IKE daemon isakmpd of OpenBSD was used. The IKE-protocol supports the following algorithms, where the default values are represented in bold:

Phase 1	
Authentication	**RSA** , PSK
Modes	**Main**, Aggressive
DH-groups	1 (768 bit key-length), **2 (1024 bit**), 5 (1536 bit)
Encryption	DES, **3DES**
Life cycle	**999.999.999 seconds**
Authentication	**SHA1**, MD5
Phase 2	
Life cycle	**Time (7200s**), limit
Encryption	DES, **3DES**, AES
Authentication	**SHA1**, MD5
PFS	yes, **no**

The implementation of the IKE protocol does not show any known security weaknesses. No known security weaknesses of the OpenBSD-Isakmpd daemon were found. Additionally, the system incorporates a VPN bridge to transport non-IP-packets through the IPsec-tunnel Broadcast and multicast packets can be transported and also ISO-protocols. The key length of 1024 bit for the DH group 2 key exchange offers sufficient protection for the next three to five years.

Using the default configuration a VPN tunnel is only established if required. To set up a VPN the security modules first exchange the necessary information about their protected nodes. If unencrypted IP communication between internal and external network is allowed, which is not the default setting, then the security module that is in the role of the client sends the first packet in plain text. The security module on the receiving side recognizes that the communication should be protected by a secure tunnel and initializes the establishing of tunnel

The use of DES as encryption algorithm is critical. In particular, in combination with the key life span of 31 years in phase 1 it is possible to break the DES key with a brute force attack (already 1999, DES was broken in a challenge in less than a day). Since the configuration tool does not set perfect-forward-secrecy (PFS) as default, the key for the ESP-protocol can then also be determined. This configuration is not recommended under security relevant aspects. The long life cycle was chosen due to the reliability of the automation network. PFS is switched off for the reason of robustness and performance. DES and MD5 as encryption and hash algorithm, respectively, were included to conform to RFC 2409, which defines IKE. After the update of RFC 2409 to RFC 4109 in May 2005, the support of DES and MD5 is no longer necessary.

3.1.2 Firewall

The security module incorporates two packet filters. The packet filter e2f that filters Ethernet packets was especially developed for the security module. The pf packet filter was adopted from OpenBSD for filtering IP packets. Here, the stateful-inspection-technology is used. The stateful-inspection-technology recognizes IP-connections and allows the filtering of these connections instead of individual packets. Packets are prioritized with Class-Based-queuing (CBQ) to ensure that there is always enough bandwidth available for administration protocols such that a denial-of-service attack is not possible. In order to avoid identification of the systems behind the security-module, the packet filter carries out a so called scrubbing of the packets.

The pf-packet filter of OpenBSD does not include any known weaknesses. A test of the filter rules set by the configuration tool does not identify any implementation failures. Also a test of the Layer-2 filter e2f revealed no security weaknesses.

3.1.3 Firmware Update

A new firmware version is provided in an encrypted way and is also digitally signed by Siemens. Hence, it was not possible to load a manipulated firmware into the device. For the encryption a global key is used that equals for all devices. Hence, with some effort is possible to compromise this encryption key by reading it out of a device. An adversary does not gain much, though, such that the encryption of the firmware is no relevant security objective.

If the secret key of Siemens is compromised that is used for signing the firmware any program could be loaded to the security device. Then, all devices need to be replaced. A mechanism to revoke certificates would be desirable for such a case, e.g. by using a so called certificate revocation list (CRL). Furthermore, the device offers a version control of the loaded firmware but does not avoid that an old version is loaded. For instance, this old version might include known security weaknesses that can be exploited. Preventing such would contradict the objective of robustness, though.

3.1.4 Operating System

The access to the security module is an SSL protected web interface. The handling and upload of the configuration files as well as the download of the logging files is carried out via that interface. A command line access is not available. No weak points could be found in the used operating system VxWorks.

3.1.5 Web Server

The security module uses an SSL web server named MiniWeb which is a development of Siemens. The web server only provides this SSL access. The MiniWeb server is based on OpenSSL and uses standard cryptographic schemes. After the login the user gets the message “Siemens AG, security module”. Further options are not available. An analysis of the configuration tool did not reveal any information about the used URLs. The certificates of the web server are generated by the configuration tool automatically. The certificates hold a 1024 bit sized key and they have a life span of around 32 years. MD5 is used as the hash function. SSL certificates can also be generated individually with other settings by an external certificate authority and loaded with the configuration tool.

The MiniWeb server is well implemented. The SSL implementation does not show any failures. The only security weakness is the long life span of the certificate and the use of MD5 for the generation of the certificates. The key length of 1024 bits is sufficient for the next three to five years.

3.1.6 Time Synchronization and Logging

The security module allows time synchronization based on the (simple-)network-time-protocol (NTP). The NTP protocol is an UDP protocol. The client requests the time from an NTP server and the server responds with its current time. Since the UDP protocol is used, the NTP protocol does not offer any protection against IP spoofing or data manipulation.

The NTP protocol neither provides authenticity nor integrity of the transferred time. A forgery of the information allows a denial-of-service-attack (DoS) on the VPN function. Hence, the NTP protocol should be used cautiously.

The logging of the time setting shows weaknesses since expired certificates and ARP spoofing attacks are not logged. Even the failure of establishing IPsec tunnels due to the expired certificates were not logged. A modification of the time is logged only when this is set manually, but not when it is set over NTP. In the default setting numerous events are not logged.

3.2 Configuration

The security module is configured by means of a security configuration tool installed on the configuration PC. This tool stores its files encrypted in a database. The configuration data is transferred from the PC to the security module in an encrypted manner with SSL. During the first configuration at initialization time a direct connection between PC and security module is necessary since the addressing of the security module is made via the MAC address. Afterwards, the communication is carried out over IP such that no direct connection is required anymore for configuring the Scalance device. Certificates and keys are then transferred to the security module by the configuration tool.

It was not possible to break the encryption of the configuration files. A man-in-the-middle attack on the encrypted SSL transfer is not possible. Since no further access to the security module is available, the communication channel between configuration PC and security module is secure.

3.2.1 Configuration Files

The configuration tool transfers the configuration data via SSL. Hence, eavesdropping of the connection and determination of the data is not possible. The analysis of the configuration files gives only information about the default settings of the firewall. The rules defined in the configuration file reveal no failures. The files are very well documented and do not show any logical mistake.

3.2.2 Bridge

The security module provides bridge functionality in order to ease installation and configuration. The bridge is in learning mode by default where it detects other network components. This is done in the same manner as a switch works with the ARP protocol. There is the possibility to switch off the learning mode and to set the MAC addresses manually. This is possible in the advanced mode only, though.

It is possible to imitate a protected node outside of the protected internal network with ARP spoofing in order to let the security module send unencrypted data. However, this attack only works if the firewall allows unprotected IP-communication between internal and external network (not default setting).

Although the bridge functionality using the learning mode eases the configuration of the VPN, this function is also the module's largest weakness. Using ARP spoofing an attacker in the local network can imitate a protected network such that the security module sends unencrypted packets to the unprotected network, or he can do a man-in-the-middle-attack. This is a weakness in principle and not especially a weak point of the security module, in particular since the default-settings prevent this attack.

4 Summary

The security module is designed for using it in an automation network in order to protect the network from data theft and manipulation as well as attacks from the external network. The reliability of the network is of first priority, the aspect of security follows right after. Furthermore, the device needs to be easy to configure. These basic assumptions are reflected in the standard settings.

The security module performs excellent under these assumptions. The module provides sufficient protection for most applications, although some weaknesses need to be accepted because of reliability. The module is easy to install and to configure such that non-IT-experts can use the device. It is possible to configure the device for almost all demands.

Altogether, we conclude that the security module reaches the high security targets. The configuration is extremely easy so that the network can be securely configured with a few settings. False settings are hardly ever possible. The automation branch requires extremely robust components so that concessions were made. On the other side the device allows setting up an all around secure network according to the current state of knowledge. A robust case rounds off the picture.

5 References

Functional Specification, Version 1.0, 7.10.2003

Security Target, Version 0.2, 31.10.2003

Instruction Handbook, 1/2005

Design Specification, 19.1.2004